IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
KNOXVILLE DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v. **CASE NO: 3:18-CR-78**

GEORGE ROBERT EVERHART,

Defendant**.**

MOTION TO SUPPRESS EVIDENCE OBTAINED FROM GOOGLE AND CHARTER COMMUNICATIONS AND TO SUPPRESS ALL EVIDENCE RESULTING FROM THOSE SEARCHES AS FRUIT OF THE POISONOUS TREE

Defendant, GEORGE ROBERT EVERHART, through counsel and pursuant to U.S. Const. amend. IV moves this Honorable Court to suppress any evidence obtained from Google and from Charter Communications and to suppress all evidence resulting from those searches as the fruit of the poisonous tree[1].

FACTS

In March, 2018, Google provided to the National Center for Missing and Exploited Children (NCMEC) multiple images and videos stored in Mr. Everhart's Google account, as well pages of IP addresses[2] and Mr. Everhart's account information. NCMEC viewed this information and then used the information to conduct its own investigation, including reviews of Facebook

[1] Mr. Everhart has requested indigent defense funding for the services of an expert in digital forensics, but is still in the process of obtaining the funding. Mr. Everhart will file a memorandum of law in support of this motion once his expert has been fully retained, has conducted his analysis and has produced his report, which Mr. Everhart intends to use to support the motion.

[2] It is unclear at this time whether the information provided contained other data that did not involve child pornography. Mr. Everhart's Google account unquestionably contained such information, including personal romantic correspondence and videos of Mr. Everhart's intimate associations with numerous adult women and this information was at some point provided to the government by Google.

accounts belong to Mr. Everhart. NCMEC also contacted ICAC in Knoxville and shared the information obtained from Google with ICAC, as well as NCMEC's investigation of that information. Officers from ICAC then served an administrative subpoena on Charter Communications for the location of the physical location of the IP Addresses provided by Google and Charter provided ICAC with Mr. Everhart's residence as the location of the IP address.

On May 30, 2018, the government sought and obtained a search warrant for Mr. Everhart's Google Account. It is unclear how much of the information eventually obtained by the government from Google, including Mr. Everhart's intimate adult associations, was obtained as a result of the search warrant or was provided by Google to NCMEC. The government did not obtain a warrant to obtain his physical location from Charter.

GROUNDS FOR THE MOTION

The Fourth Amendment enshrines a promise that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. The contours of this right when it comes to data and electronically stored information are still evolving. From its plain language, the Fourth Amendment protects security and although privacy is undoubtedly an aspect of security, security is a broader concept than privacy. The Court has increasingly acknowledged this distinction in regard to electronically stored information:

> The "basic purpose of this Amendment," our cases have recognized, "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 528, 87 S.Ct. 1727, 18 L.Ed.2d 930 (1967). The Founding generation crafted the Fourth Amendment as a "response to the reviled `general warrants' and `writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley v. California*, 573 U.S.

> ___, ___, 134 S.Ct. 2473, 2494, 189 L.Ed.2d 430 (2014). In fact, as John Adams recalled, the patriot James Otis's 1761 speech condemning writs of assistance was "the first act of opposition to the arbitrary claims of Great Britain" and helped spark the Revolution itself. Id., at ___ - ___, 134 S.Ct., at 2494 (quoting 10 Works of John Adams 248 (C. Adams ed. 1856)).

Carpenter v. U.S., 138 S. Ct. 2206, 2213 (2018).

Thus, in *Carpenter v. U.S.*, the Supreme Court recently held that cell site location data was subject to the Fourth Amendment's warrant requirement, although it was in the possession of a third party, who had provided it in response to a court order. *Carpenter*, 138 S. Ct. at 2211 -2221. In so holding, the Court observed:

> the [Fourth] Amendment seeks to secure "the privacies of life" against "arbitrary power." *Boyd v. United States*, 116 U.S. 616, 630, 6 S.Ct. 524, 29 L.Ed. 746 (1886). Second, and relatedly, that a central aim of the Framers was "to place obstacles in the way of a too permeating police surveillance." *United States v. Di Re*, 332 U.S. 581, 595, 68 S.Ct. 222, 92 L.Ed. 210 (1948).
>
> We have kept this attention to Founding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools. As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to "assure[ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo v. United States*, 533 U.S. 27, 34, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001).

Id. at 2214.

Indeed, the Court has long held that the fact that highly sensitive information is held by a third party does not automatically defeat an individual's expectation of privacy or remove from the ambit of the Fourth Amendment a disclosure of such information by a third party to the government. See, e.g., *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (patients have a reasonable expectation of privacy in test results performed and held by a hospital); B*ond v. United States*, 529 U.S. 334, 338–39 (2000) (passengers retain an expectation of privacy in luggage

placed in the overhead bin of a bus even though there is a possibility that the luggage will be inspected by others); S*toner v. California*, 376 U.S. 483, 489–90 (1963) (hotel guests do not forfeit protection under the Fourth Amendment even though their rooms belong to the hotel and they provide "implied or express permission" for third parties to access their rooms). Indeed, the Court's precedents make clear that even where the sensitive information is located in spaces owned by third parties, the third party does not have authority to open the space to law enforcement. E.g., *Lustig v. United States*, 338 US 74 (1949) (holding that hotel manager did not have authority under the Fourth Amendment to give key to hotel guest's room to law enforcement officers). As the Court's decisions in *Carpenter*, *United States v. Jones*, 565 U.S. 400 (2012), and *Riley v. California*, 134 S. Ct. 2473 (2014), illustrate, the innovations of the digital age preclude the wooden extension of analog-era precedents where technology has greatly increased the government's ability to obtain intimate information.

As the Court made clear in *Jones*, "the *Katz* reasonable-expectation-of-privacy test has been added to, not substituted for," property-based conceptions of Fourth Amendment rights. *Jones*, 565 U.S. at 409; see also *Florida v. Jardines*, 133 S. Ct. 1409, 1415-16 (2013). In the digital age, people live virtual as well as physical lives. They use computers, smart phones and the internet to conduct business, social interactions and to generate and store vast quantities of data. On the internet they engage in various types of protected speech including anonymous political speech.

When people access the internet and move to particular sites on the internet, they leave a trace of their physical location in the form of an IP address that corresponds to their physical location. Through the acquisition of a person's IP address, it is possible to track the person's virtu-

al movements throughout the internet, and to link the person with his or her online activities, including with anonymous political speech. The ability of the government to track a person's virtual movements through the acquisition of an IP address and its corresponding physical location is more intrusive than the ability to track a person's physical movements at issue in *Carpenter,* because it reveals specific details about a person's personal, political and intimate associations. With an IP address and its physical location, it is possible, for instance, to identify the residence or location of the sender of an anonymous political post, which surely would have concerned the Founders, who often wrote anonymously.

Prior to *Carpenter,* the Court recognized that the government may not use technology to track a person's physical activities in his or her home. *Kyllo v. United States*, 533 US 27 (2001). There is no compelling reason, therefore, that the government should be allowed to track a person's virtual activities in his or her home, especially given that those virtual activities are likely to reveal much more about a person's associations, preferences, religious beliefs, intimate relations, friendships, interests, financial activities and cetera than the thermal imaging device at issue in *Kyllo*, which would have revealed only "how warm—or even how relatively warm—Kyllo was heating his residence." *Kyllo*, 533 U.S. at 38. If the Court in *Kyllo* was concerned that a technological device might reveal "at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider 'intimate,'" *id.* at 38, it is surely reasonable to conclude that the Court would consider even more worrisome a technology that could reveal that the woman purchased dandruff shampoo, bubble bath, a rubber ducky, a shower curtain depicting pink flying toy ponies or that she shared with her married lover a photograph of her naked bubble coated legs. As the Court noted in *Carpenter,*

> we rejected in *Kyllo* a "mechanical interpretation" of the Fourth Amendment and held that use of a thermal imager to detect heat radiating from the side of the defendant's home was a search. *Id.*, at 35, 121 S.Ct. 2038. Because any other conclusion would leave homeowners "at the mercy of advancing technology," we determined that the Government — absent a warrant — could not capitalize on such new sense-enhancing technology to explore what was happening within the home. Ibid.

Carpenter, 138 S. Ct. at 2214.

The Court also reaffirmed in *Carpenter* that the government cannot use a subpoena or court order as a substitute for a warrant. *Id* at 2221 - 2222.

In *Riley v. California,* the Court recognized that the considerable privacy concerns in the search of a cellphone extended beyond the phone itself:

> [T]he data a user views on many modern cell phones may not in fact be stored on the device itself . . . . [The device may be] used to access data located elsewhere, at the tap of a screen. That is what cell phones, with increasing frequency, are designed to do by taking advantage of "cloud computing. Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference. See Brief for Electronic Privacy Information Center in No. 13-132, at 12-14, 20. Moreover, the same type of data may be stored locally on the device for one user and in the cloud for another.

Riley, 134 S. Ct. at 2491.

In Riley, the Court acknowledged the extent and intimacy of the data stored on cell phones and in the cloud, which far exceeds anything a person would or could store in his or her actual home. Id at 1290 -1. If as the Court acknowledged in *Riley,* access to the data on a phone requires a warrant regardless of whether the data is located on the device or in the cloud, then it stands to reason that a third party entrusted with that data, in effect a person's virtual home and virtual life, could not give the government access to that data anymore than a hotel manager could give the government a key to a person's hotel room. E.g., *Lustig v. United States*, 338 US 74 (1949). The

Court's jurisprudence has evolved to take account of the right of the people, including Mr. Everhart, to be secure in their digital papers and effects even when held or produced by third parties and has expressly limited and abrogated analog era precedents that did not and indeed could take into account or anticipate the realities of the digital world.

Although the government did eventually obtain a search warrant for Mr. Everhart's Google account, the warrant[3] is overly broad in its language and overly broad in its results. U.S. CONST. amend. IV (requiring a warrant to "particularly describe[e] the place to be searched, and the persons or things to be seized."); *Ashcroft v. al-Kidd,* 131 S. Ct. 2074, 2084–85 (2011) (discussing the particularity requirement's role in preventing the use of general warrants). The warrant does not seek merely evidence of child pornography in the account, but the production of the entirety of Mr. Everhart's account, including his correspondence. The information currently possessed by the government and obtained from Google includes a vast quantity of information pertaining to Mr. Everhart's intimate adult relationships, economic activity, employment, familial relationships and associations that is not criminal in nature or related to the production and distribution of child pornography. The warrant is also the fruit of the initial warrantless search of Mr. Everhart's Google account, because the basis for the warrant is grounded in that initial warrantless search.

Mr. Everhart had the right to be secure in his digital papers and effects from government intrusions and the government had the obligation to obtain a warrant for that data supported by probable cause that described the data sought with particularity. The government failed to do so and accordingly, the information obtained and its fruits must be suppressed.

---

[3] Because the warrant contains potentially identifying information regarding the children, Mr. Everhart will file a motion to file the warrant under seal.

Respectfully submitted this the 14th day of November, 2018.

_/s/T. Scott Jones__

T. Scott Jones
Gena Lewis
BANKS & JONES
2125 Middlebrook Pike
Knoxville, TN 37921
Office Phone: (865) 546-2141
Fax: (865) 546-5777

Counsel for Defendant George Robert Everhart

CERTIFICATE OF SERVICE

I, T. Scott Jones, counsel for Plaintiff hereby certify that on November 14, 2018, I served a copy of the foregoing pleading or document through CM/ECF which will serve all counsel of record.

Respectfully submitted,

_/s/T. Scott Jones__